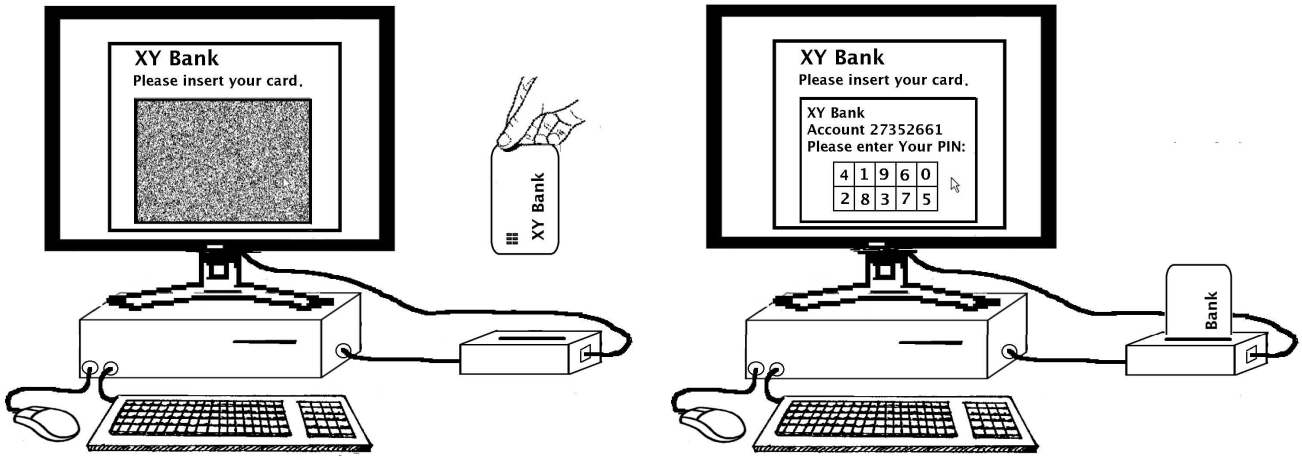
**Arbeitsbereich Theoretische Informatik** 24.3.2012

Themenvorschlag für eine Abschluss-Arbeit (Bachelor, Master etc.)

# Trojanersichere Fenster: Verschlüsselung/Entschlüsselung

Online Accounts, wie z.B. Online Bankkonten oder Online Unternehmenszugänge, sind nicht abhörsicher: ein auf den Rechner des Benutzers eingeschleppter Trojaner-Virus kann die vom Server an den Klienten geschickten Informationen heimlich aufnehmen, z.B. durch screen shots oder screen movies, und selber weiterverarbeiten oder an seinen Master schicken. Darüberhinaus kann der Trojaner auch die Informationen abhören, die vom Klienten an den Server geschickt werden: durch Beobachtung der Tastatur und der Mausbewegungen. Insbesondere kann der Trojaner das Account Passwort abhören, wenn es eingegeben wird.

Durch das "Sichere Fenster" Verfahren kann dieses Abhören - in beiden Richtungen - verhindert werden. Benötigt wird ein Gerät, das zwischen den Bildschirmausgang am Rechner und den Bildschirm geschaltet wird. Das Gerät hat idealerweise einen Smartkarten-Leser, damit mehrere Online Accounts bedient werden können. Wenn sich der Benutzer in seinen Online Account einloggen möchte, wird ihm nach der Angabe seines login-Namens vom Server ein Teil des Bildschirms kodiert übertragen, so dass dort nur ein Rauschen zu sehen ist. Nach Einstecken der Smartkarte in das Gerät wird der kodierte Teil des Bildschirms dekodiert, der Rest bleibt unverändert. Die Dekodierung wird dabei durch ein paar Pixel des an den Bildschirm gesendeten Bildsignals gesteuert.




Durch dieses Prinzip ist schon mal garantiert, dass die in dem "Sicheren Fenster" stehenden Informationen vom Server an den Klienten nicht durch einen Trojaner abgehört werden können. Aber es können auch Informationen vom Klienten an den Server unabhörbar übertragen werden, und zwar durch Betätigen von beschrifteten Schaltflächen, deren Beschriftungen erst nach der Dekodierung für den Benutzer sichtbar werden und deshalb für einen Trojaner unsichtbar sind. A

Das von der Univ. Tübingen zur Patentierung angemeldete Verfahren soll durch mehrere Abschluss-Arbeiten (Bachelor, Master, etc.) stufenweise implementiert werden.

In der hier beschriebenen Teilaufgabe "Verschlüsselung/Entschlüsselung" soll Software konzipiert und entwickelt werden, die ein gegebenes png Bild des Browserfensters verschlüsselt und dann einen png Screenshot des gesamten Bildschirms wieder entsprechend entschlüsselt. Weil bei der Entschlüsselung (in der Box) die Performanz entscheidend ist, soll diese maschinennah programmiert werden. Die Verschlüsselungsaufgabe soll dagegen in einer Programmiersprache geschrieben werden, die bei Webservern verbreitet ist. Ein Teil der Aufgabe besteht darin, die optische Verwaltungsinformation am Sicheren Fenster (für die Entschlüsselung in der Box) sinnvoll und effektiv festzulegen. Es reicht, die Entschlüsselungs-Software auf dem PC zu simulieren - die Übertragung der Entschlüsselungs-Software auf eine Hardware für die Box gehört nicht zur Aufgabe.

Betreuer: Dr. Bernd Borchert
http://www-fs.informatik.uni-tuebingen.de/~borchert/Troja/